Transforming MCT Circuits to NCVW Circuits

Zahra Sasanian and D. Michael Miller*

Department of Computer Science, University of Victoria
Victoria, BC, Canada V8W 3P6
{sasanian,mmiller}@uvic.ca

Abstract. Mapping a circuit of reversible gates to a circuit of elementary quantum gates is a key step in synthesizing quantum realizations of Boolean functions. The library containing NOT, controlled-NOT and controlled square-root-of-NOT gates has been considered extensively. In this paper, we extend the library to include fourth-root-of-NOT gates. Experimental results using REVLIB benchmark circuits show that using this extended library results in smaller quantum circuits.

1 Introduction

Many reversible circuit synthesis methods have been presented in the literature. A good review can be found in [10]. Most methods produce a circuit composed of a cascade of basic reversible gates. After, or sometimes during, synthesis the reversible gates are mapped to elementary quantum gates implemented in the target technology, a step analogous to technology-mapping in traditional digital circuit design. Much of the work in this area has focused on the quantum gate library of NOT, controlled-NOT, controlled-V and controlled-V^+ gates, which is termed the NCV library. The last two are *square-root-of-NOT* gates. The work here extends the library to include controlled-W and controlled-W^+ gates which are *fourth-root-of-NOT* gates. The question we seek to address is to what extent the NCVW library will yield smaller quantum circuits.

Although the paper concentrates on MCT reversible gates, the proposed methods can be applied to other reversible gates, *e.g.* Fredkin [2] gates, by transforming them to Toffoli gate realizations. The approach can also be targeted to other quantum gate libraries.

All circuits described in this paper have been verified using the QMDD circuit equivalence checker described in [11]. The NCV and NCVW catalogs of circuit realizations for MCT gates, the programs that generate those catalogs and the MCT to quantum circuit mapping program (in Python) are available from the authors.

The rest of the paper is organized as follows. Section 2 gives the necessary background. Section 3 outlines an approach to finding NCVW realizations of single MCT gates, and Section 4 shows how that work can be used in finding

* This work was supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

A. De Vos and R. Wille (Eds.): RC 2011, LNCS 7165, pp. 77–88, 2012.

NCVW realizations of MCT circuits. Experimental results are given in Section 5 and the paper finishes with conclusions and suggestions for ongoing work in Section 6.

2 Background

We here present the background necessary for this paper. Readers interested in a more detailed introduction should consult the literature.

Definition 1. *A multiple-output Boolean function is* **reversible** *if it maps each input assignment to a unique output assignment.*

A reversible function is realized by a cascade of reversible gates with no fan-out or feedback [5]. A completely or incompletely-specified irreversible function can be embedded into a reversible function, usually with more inputs and outputs, and then realized by a reversible circuit [3].

Definition 2. *A* **multiple-control Toffoli** *(MCT) gate with* **target line** x_j *and* **control lines** $\{x_{i_1}, x_{i_2} \cdots x_{i_k}\}$*, maps* $(x_1 \ldots x_j \ldots x_n)$ *to*

$$(x_1 \ldots (x_{i_1} x_{i_2} \cdots x_{i_k}) \oplus x_j \ldots x_n).$$

Note that all controls must be 1 for the target to be inverted. An MCT gate with no control is the well-known **NOT** *gate. An MCT gate with a single control line is called a* **controlled-NOT** *(CNOT) gate. We use* $T(C;t)$ *to denote the MCT gate with* C *being the set of controls and* t *being the target.*

Note that for all circuits considered in this work, MCT gate controls and controls for the quantum gates discussed below must have binary (0 or 1) and not quantum values.

Fredkin gates [2], Peres and inverse-Peres gates [6] are also used in reversible circuits. Each such gate can be substituted by an equivalent sequence of MCT gates. Indeed, any reversible gate can be substituted by a sequence of MCT gates. A reversible circuit composed of only MCT gates is thus used as the starting point for the approach presented in this paper.

Many quantum gates have been defined and studied in the literature [5]. Here we consider what we term the NCVW library which consist of the NOT and $CNOT$ gates given above and four single-control gates (V,V^+,W,W^+) defined below.

It is well known (see [5] for details) that the operation of each gate in an n-line reversible or quantum circuit can be represented by a square matrix of dimension 2^n. The construction of the matrix depends on which line is the target, which lines are the control(s) and a 2×2 matrix defining the operation on the target line. For example, the target matrix for an MCT gate, including NOT and $CNOT$, is $\mathbf{N} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Theorem 1. *Consider the matrix*

$$\mathbf{R}_k = \frac{1}{2}\begin{pmatrix} 1+i^{2/k} & 1-i^{2/k} \\ 1-i^{2/k} & 1+i^{2/k} \end{pmatrix} \tag{1}$$

where k is a power of 2. $\mathbf{R}_k$ is a k-th root of $\mathbf{N}$, i.e. $(\mathbf{R}_k)^k = \mathbf{N}$.

Proof: Consider

$$\mathbf{R}_p \times \mathbf{R}_p = \frac{1}{2}\begin{pmatrix} 1+i^{2/p} & 1-i^{2/p} \\ 1-i^{2/p} & 1+i^{2/p} \end{pmatrix} \times \frac{1}{2}\begin{pmatrix} 1+i^{2/p} & 1-i^{2/p} \\ 1-i^{2/p} & 1+i^{2/p} \end{pmatrix} \tag{2}$$

$$= \frac{1}{2}\begin{pmatrix} 1+i^{4/p} & 1-i^{4/p} \\ 1-i^{4/p} & 1+i^{4/p} \end{pmatrix} \tag{3}$$

The matrix in Equation 3 is $\mathbf{R}_{p/2}$ which is verified by setting $k = p/2$ in Equation 1. Since $\mathbf{R}_p \times \mathbf{R}_p = \mathbf{R}_{p/2}$ and $\mathbf{R}_1 = \mathbf{N}$, it follows by induction that for k a power of 2, $(\mathbf{R}_k)^k = \mathbf{N}$. □

Corollary 1.1 Since the conjugate of the product of two matrices is the product of their conjugates, $(\overline{\mathbf{R}}_k)^k = \mathbf{N}$.

Let $\mathbf{V} = \mathbf{R}_2 = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$. Clearly, $\mathbf{V} \times \mathbf{V} = \mathbf{N}$. Let $\mathbf{V}^+$ be the conjugate transpose (adjoint) of $\mathbf{V}$. It follows from Corollary 1.1 that $\mathbf{V}^+ \times \mathbf{V}^+ = \mathbf{N}$. further, it is readily verified that $\mathbf{V}^+ = \mathbf{V}^{-1}$.

Definition 3. *A **controlled-**V gate applies the transformation defined by the matrix $\mathbf{V}$ when the single control line has value 1. Likewise, a **controlled-**V^+ gate applies the transformation defined by the matrix $\mathbf{V}^+$ when the single control line has value 1. Both gates are called **square-root-of-NOT** gates. They both pass the target line value through unaltered if the control has value 0.*

Definition 4. *A **controlled-controlled-**V gate is the extension of the controlled-V gate to the case of two controls both of which must be 1 to apply the transformation to the target. A **controlled-controlled-**V^+ gate is the analogous extension to the controlled-V^+ gate.*

Let $\mathbf{W} = \mathbf{R}_4 = \frac{1}{2}\begin{pmatrix} 1+\sqrt{i} & 1-\sqrt{i} \\ 1-\sqrt{i} & 1+\sqrt{i} \end{pmatrix}$. Its adjoint is $\mathbf{W}^+ = \frac{1}{2}\begin{pmatrix} 1-i\sqrt{i} & 1+i\sqrt{i} \\ 1+i\sqrt{i} & 1-i\sqrt{i} \end{pmatrix}$. By definition, $\mathbf{W} \times \mathbf{W} = \mathbf{V}$. It follows directly that $\mathbf{W}^+ \times \mathbf{W}^+ = \mathbf{V}^+$. It is readily verified that $\mathbf{W}^+ = \mathbf{W}^{-1}$.

Definition 5. *A **controlled-**W gate applies the transformation defined by the matrix $\mathbf{W}$ when the single control line has value 1. Likewise, a **controlled-**W^+ gate applies the transformation defined by the matrix $\mathbf{W}^+$ when the single control line has value 1. Both gates are called **fourth-root-of-**NOT gates.*

The quantum bit operations corresponding to the matrices V, V^+, W and W^+ are rotations around the x-axis of the Bloch sphere [5]. V and W define

rotations by 90° and 45° in one direction while V^+ and W^+ define rotations by 90° and 45° in the opposite direction. Considering computation, we note from the well-known De Moivre's theorem that $i^{1/k} = \cos\frac{\pi}{2k} + i\sin\frac{\pi}{2k}$. Hence $\sqrt{i} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$.

The above can be extended to gates implementing other roots-of-NOT. Higher order roots require progressively smaller rotation angles. We do not consider that option here and, for that reason, we do not consider the case of two-control W and W^+ gates.

The following properties and definitions are useful for simplifying circuits.

Property 1. MCT gates, including NOT, CNOT and Toffoli gates, are self-inverse and two identical such gates in a row yield the identity mapping. V and V^+ gates with the same target and the same control are the inverse of each other. W and W^+ gates with the same target and the same control are the inverse of each other.

Property 2. Given a cascade of gates $G_1 G_2 \ldots G_k$ realizing the reversible function F, the cascade $G_k^{-1} \ldots G_2^{-1} G_1^{-1}$ realizes the function F^{-1}, where G_i^{-1} is the inverse gate for G_i.

Definition 6. *Since an MCT gate is self-inverse applying Property 2 to a realization of the gate yields an alternate realization for the same gate. We term this the* **reverse** *realization.*

Property 3. In a circuit realizing a reversible function, the functionality is not changed if for any line, (a) all V gates are replaced by V^+ gates and all V^+ gates are replaced by V gates, or (b) all W gates are replaced by W^+ gates and all W^+ gates are replaced by W gates, where both interchanges must be applied to any line that contains both V-type and W-type gates.

Property 3 is the observation that we can reverse the direction of rotation in the Bloch sphere so long as we do it consistently.

The methods discussed below produce circuits composed of NOT, $CNOT$, and controlled-V, V^+, W and W^+ gates. We term such circuits NCVW circuits. We compare our results to NCV circuits which are similar except they contain no controlled-W or controlled-W^+ gates.

Definition 7. *The* **cost** *of an NCVW or NCV circuit is taken to be the number of gates,* i.e. *we assume NOT, CNOT and single control quantum gates all have cost 1.*

For drawing circuits, we follow the normal conventions of using a $\oplus$ for an MCT gate or a box containing the gate name to indicate the operation performed on the target line, and a $\bullet$ to indicate each control connection.

3 NCVW Circuits for MCT Gates

It is well known [1] that the Toffoli gate $T(\{c, b\}; a)$ can be realized using 5 NCV gates as shown in Figure 1(a). This extends to realizing controlled-controlled-V

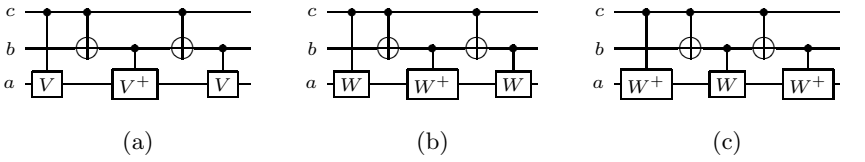

Fig. 1. (a) NCV realization of $T(\{c, b\}; a)$. (b) NCW realization of $V(\{c, b\}; a)$. (c) NCW realization of $V^+(\{c, b\}; a)$.

and V^+ gates using NCW gates as shown in Figure 1(b) and (c), respectively. Note that the circuit in Figure 1(a) represents 4 distinct realizations since it can be reversed and V and V^+ can be interchanged. The circuits in Figure 1(b) and (c) each represent two realizations by reversal.

Consider realizing $T(\{d, c, b\}; a)$. The circuit in Figure 2(a) is found by adding line d to the circuit in Figure 1(a). The correct operation of this circuit is readily verified by considering the cases of $d = 0$ and $d = 1$ in turn.

The circuit in Figure 2(b) is derived from 2(a) by (i) substituting an instance of the circuit in Figure 1(b) for the $V(\{d, c\}; a)$ gate, (ii) substituting a reversed instance of the circuit in Figure 1(c) for the $V^+(\{d, b\}; a)$ gate, and (iii) substituting an instance of the circuit in Figure 1(b) for the $V(\{d, b\}; a)$ gate. Note that once substituted two gates from (ii) cancel with two gates from (iii). Hence the gates $V^+(\{d, b\}; a)$ and $V(\{d, b\}; a)$ map to 3 gates each in the reduced circuit. The circuit in Figure 2(b) is the circuit given by Barenco *et al.* [1]. The construction shown here is quite different.

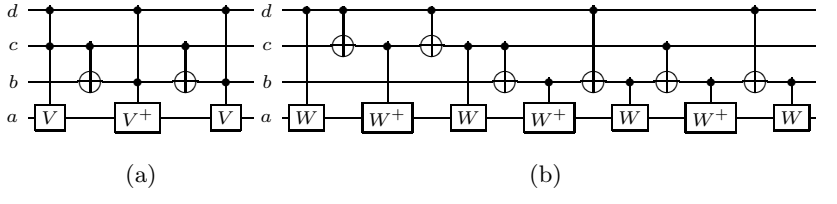

Fig. 2. (a) NCV realization of $T(\{d, c, b\}; a)$. (b) NCW circuit for $T(\{d, c, b\}; a)$.

In [7], we have shown how to decompose an MCT gate into a circuit composed of controlled-W, controlled-W^+ and MCT gates with fewer controls. An example for 7 controls and 1 ancillary line (labeled 1) is shown in Figure 3. Using the general form of this decomposition and using the circuits in Figures 1(b), 1(c) and 2(b) it is possible to build a catalog of MCT realizations for any number of controls. Further, separate circuits can be derived for differing numbers of available ancillary lines. See [7] for details.

Table 1(a) shows the costs of the NCVW realizations of MCT gates for up to 20 controls. Note that no NCVW realizations exist for 0 ancillary lines and greater than 3 controls. A blank entry at the right end of a row means the cost

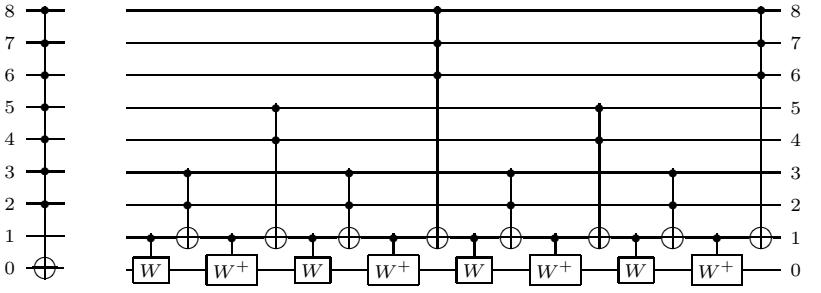

Fig. 3. Example Decomposition of a 7-control MCT Gate

can not be reduced by adding another ancillary line. For comparison, Table 1(b) shows the costs of NCV realizations of MCT gates as presented in [4]. Note that the NCVW are consistently cheaper and for 3 controls and 7 or more controls one less ancillary line is required to achieve the smallest circuit.

4 NCVW Circuits for MCT Circuits

The previous section addressed finding an NCVW realization for a single MCT gate and how that can be used to build a catalog of NCVW realizations for individual MCT gates with particular numbers of controls and ancillary lines. Here, we consider how such a catalog can be used in transforming a MCT gate circuit to an NCVW circuit. The approach described here is similar to the one presented in [8]. The difference is that it uses NCVW realizations of MCT gates developed in [7] in place of NCV realizations. We outline the approach below. Readers interested in full details should consult the references.

Our procedure to map a MCT circuit to a NCVW circuit uses a **Line Labeling Procedure** (Procedure 1 of [8]) and the **Gate Reduction Procedure** (Procedure 2 of [8]). Both are applicable to MCT and quantum gates. The Line Labeling Procedure traverses a circuit assigning labels to line segments such that two segments on the same line that are assigned the same label have identical functionality. This is done by identifying gate sequences that realize the identity function using a stack of gates for each circuit line. The Gate Reduction Procedure finds possible cancelations and reductions in the circuit by moving gates across the circuit and making them adjacent to every gate in their movement domain. It starts from one end of the circuit and labels one gate at a time. Then it moves that gate back through the circuit as far as possible to find the best reduction. The gate either may be canceled with its inverse or may be reduced to a single gate when combined with other gates.

The key extension to the Gate Reduction Procedure as given in [8] to incorporate W and W^+ gates, was to modify the gate combining step so that it considers more than two gates at a time to find possible reductions. As a gate (G_p) is moved across the circuit, a list is made that contains gates that can be

Table 1. Cost of MCT gate circuits: (a) NCVW cost, (b) NCV cost

	Number of Ancillary Lines							
Controls	0	1	2	3	4	5	6	7
0	1							
1	1							
2	5							
3	13							
4		20						
5		28						
6		40						
7		52						
8		64						
9		80	76					
10		96	88					
11		112	104	100				
12		128	120	112				
13		152	136	128	124			
14		176	158	144	136			
15		200	176	160	152	148		
16		224	200	176	168	160		
17		248	224	200	184	176	172	
18		272	248	224	200	192	184	
19		296	272	248	224	208	200	196
20		320	296	272	248	224	216	208

(a)

	Number of Ancillary Lines								
Controls	0	1	2	3	4	5	6	7	8
0	1								
1	1								
2	5								
3		14							
4		20							
5		32							
6		44							
7		64	56						
8		76	68						
9		96	88	80					
10		108	100	92					
11		132	120	112	104				
12		156	132	124	116				
13		180	156	148	136	128			
14		204	180	172	148	140			
15		228	204	198	172	160	152		
16		252	228	222	196	172	164		
17		276	252	246	222	196	184	176	
18		300	276	270	246	220	196	188	
19		324	300	294	270	246	220	208	200
20		348	324	318	294	270	244	220	212

(b)

adjacent to G_p and have the same target and control as G_p with the same labels on their controls. Then, the gates in this list are removed from the circuit and an optimized equivalent sequence is inserted in the position of the left-most removed gate in the circuit. For example a sequence of VNW^+ gates will be replaced by NW. The optimized equivalent sequence may be empty which indicates that the corresponding set of gates realizes the identity function.

The MCT to NCVW mapping procedure is similar to Procedure 4 in [8]. It first optimizes the MCT cascade using the Gate Reduction Procedure described above. Then, MCT gates are expanded to their equivalent NCVW cascades pairwise to find optimizations across gate boundaries. To achieve this, an MCT gate is made adjacent to all other MCT gates in its movement domain and the pair that introduces the most reduction when expanding to its NCVW realization is selected. In pairwise expansion, alternative NCVW realizations such as reverse realizations, $V - V^+$, and $W - W^+$ substitutions are examined to find the best reduction. At the last step of the mapping procedure, the resulting NCVW circuit is optimized using the Gate Reduction Procedure.

Figure 4 shows the results of applying the above procedures for the NCV and NCVW libraries for the REVLIB benchmark circuit decod24-v1_24. The MCT circuit from REVLIB is shown in Figure 4(a). The NCV circuit is shown in

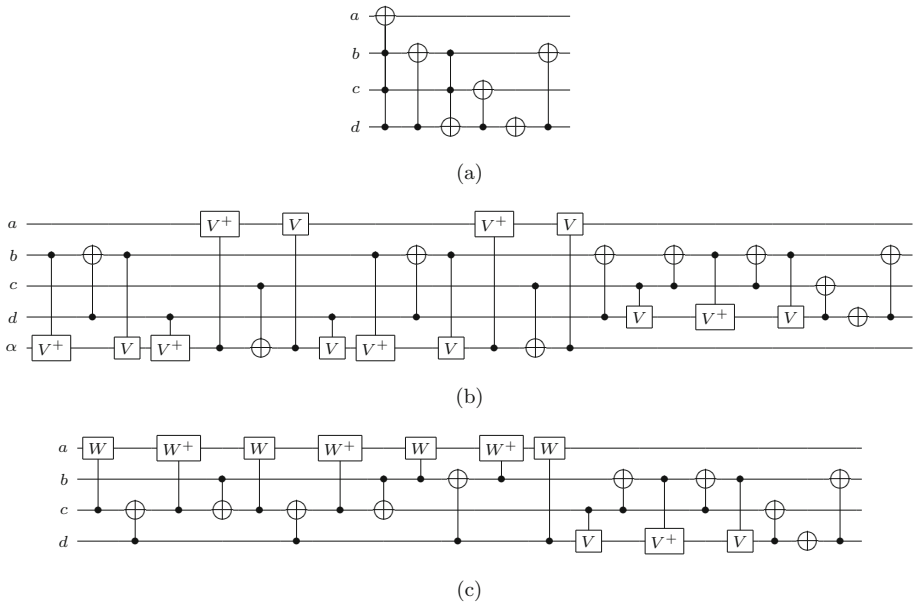

Fig. 4. Example decod24-v1_24 circuits: (a) MCT from REVLIB [9], (b) NCV, (c) NCVW

Figure 4(b) and the NCVW circuit is shown in Figure 4(c). The NCV circuit has a cost of 23 while the NCVW circuit has a cost of 20. The NCV circuit uses an added ancillary line labeled α. The NCVW does not need an ancillary line. This is because the widest gate in the MCT circuit has 3 controls and as shown in Table 1 such a gate has a 13 gate NCVW realization with no ancillary line. For a MCT circuit with more than 4 lines with a gate using all lines, an added ancillary line is required in an NCVW circuit.

The leftmost 14 gates in Figure 4(b) are an NCV realization of the $T(\{d, c, b\}; a)$ gate in 4(a). They are followed by the $T(d; b)$ gate and then by a five gate realization of the $T(b, c; d)$ in 4(a). Lastly, the final three gates in 4(a) are copied over to 4(b).

Figure 4(c) is constructed in a similar way. The first 12 gates are from the 13 gate NCVW realization of $T(a, b, c; d)$. The 13^{th} gate does not appear as it is $T(d; b)$ and cancels with the existing occurrence of that gate in Figure 4(a). The final 8 gates in Figure 4(c) are the same as in Figure 4(b).

5 Experimental Results

We have implemented the methods described above using Python 2.6.5. The circuits considered are from the REVLIB web site [9]. Our experiments were run on a system with a 3.2 GHz i5-650 CPU and 3.0 GB RAM.

Table 2. NCVW realizations of selected REVLIB benchmarks

REVLIB Circuit	REVLIB Cost	Initial Cost	MCT Gate Reduction	Quantum Gate Substitution	Quantum Gate Reduction	% Cost Reduction	CPU (sec.)
sym9_148	4368	3612	665	665	659	84.91	25.906
sym6_145	777	543	203	201	199	74.39	4.719
plus63mod8192_164*	45025	22208	19318	18863	18856	58.12	109.157
plus63mod4096_163*	32539	16808	14322	13820	13813	57.55	81.984
plus127mod8192_162*	73357	41002	35550	34193	34178	53.41	218.672
rd32-v0_66	12	12	12	8	6	50.00	0.047
rd32-v1_68	13	13	13	9	7	46.15	0.078
4gt4-v0_73*	89	80	48	48	48	46.07	0.485
rd53_133	128	104	86	78	72	43.75	0.937
cycle10_2_110	1202	694	694	682	682	43.26	3.250
hwb8_114*	14699	9131	8888	8392	8378	43.00	142.516
hwb8_115*	14691	9131	8888	8392	8378	42.97	142.906
hwb8_113*	16530	10736	10282	9804	9787	40.79	78.500
hwb8_118*	16522	10736	10282	9804	9787	40.76	78.469
hwb9_123*	22510	13494	13492	13456	13434	40.32	185.672
rd53_134	120	104	86	78	72	40.00	0.922
ham15_107	1831	1509	1184	1115	1107	39.54	14.188
hwb9_119*	44714	29842	29010	27389	27340	38.86	272.609
hwb9_121*	44665	29805	28982	27359	27311	38.85	258.141
hwb9_120*	44702	29842	29010	27389	27340	38.84	260.406
hwb9_122*	44653	29805	28982	27359	27311	38.84	257.672
4gt12-v0_86*	58	49	38	36	36	37.93	0.328
4gt12-v0_87*	54	45	34	34	34	37.04	0.187
4gt4-v0_72*	54	45	34	34	34	37.04	0.281
hwb7_59*	5236	3772	3613	3363	3352	35.98	58.438
hwb8_116*	7015	4547	4547	4505	4496	35.91	108.171
hwb8_117*	7013	4547	4547	4505	4496	35.89	108.219
4mod5-v1_22	9	9	9	7	6	33.33	0.047
4mod5-v1_23	24	24	18	16	16	33.33	0.172
peres_9	6	6	6	4	4	33.33	0.015
hwb7_60*	4170	2966	2844	2838	2829	32.16	30.234
4mod5-v0_18	25	25	19	17	17	32.00	0.141
4mod5-v0_19	13	13	10	9	9	30.77	0.047
mod5mils_65	13	13	10	9	9	30.77	0.093
mod5mils_71	13	13	10	9	9	30.77	0.094
toffoli_double_4	10	10	7	7	7	30.00	0.078
hwb7_61*	3876	2974	2906	2743	2731	29.54	41.891
hwb6_57*	1171	913	845	836	833	28.86	7.671
hwb7_62*	2611	1901	1901	1884	1878	28.07	18.719
rd53_138	44	44	44	35	32	27.27	0.594
4gt12-v0_88*	41	32	32	30	30	26.83	0.172
hwb6_56*	1530	1227	1204	1126	1122	26.67	17.656
rd32-v0_67	8	12	12	8	6	25.00	0.047
rd53_135	77	71	68	59	58	24.68	1.313
hwb4_49*	65	65	57	51	49	24.62	0.438
rd53_131	119	101	95	91	90	24.37	1.125
4gt4-v0_80*	37	28	28	28	28	24.32	0.172
rd73_140	76	76	76	61	58	23.68	1.016
sys6-v0_111	72	72	72	59	55	23.61	1.141
rd53_132	117	101	95	91	90	23.08	1.125
alu-v2_31	101	101	84	78	78	22.77	0.578
rd53_136	75	71	68	59	58	22.67	1.297
4gt4-v0_79*	49	40	40	38	38	22.45	0.375
4mod5-v0_20	9	9	9	7	7	22.22	0.047
decod24-v0_38	18	18	18	14	14	22.22	0.047
decod24-v2_43	18	18	18	14	14	22.22	0.079
ham3_102	9	9	9	7	7	22.22	0.031
hwb4_50*	63	65	57	51	49	22.22	0.437
rd32-v1_69	9	13	13	9	7	22.22	0.062
3_17_13	14	14	14	11	11	21.43	0.125
4gt4-v0_78*	53	44	44	44	42	20.75	0.265
ham15_108	453	387	378	362	360	20.53	5.485
4gt12-v1_89*	45	36	36	36	36	20.00	0.156
fredkin_6	15	15	15	13	12	20.00	0.031
ham3_103	10	10	10	8	8	20.00	0.047
rd84_142	112	112	112	94	90	19.64	2.640
sym9_146	108	108	108	88	87	19.44	1.422
mod5d2_70	16	16	13	13	13	18.75	0.109
4mod7-v0_94	38	38	38	32	31	18.42	0.125
4mod7-v0_95	38	38	38	32	31	18.42	0.125
mod5adder_127	125	107	107	104	102	18.40	1.266
mod5d1_63	11	11	11	10	9	18.18	0.078
4mod7-v1_96	39	39	39	33	32	17.95	0.188
rd53_130	232	196	196	192	191	17.67	2.579
4gt4-v1_74*	57	48	48	47	47	17.54	0.218
4_49_16*	60	60	57	53	50	16.67	0.406
4gt13_91	30	30	27	25	25	16.67	0.157
one-two-three-v0_98	40	40	40	34	34	15.00	0.187
	458551	284605	264825	253107	252662	44.90	2555.423

Table 3. Benchmarks for which the NCVW cost is greater than the NCV cost

REVLIB Circuit	NCV Cost [8]	NCVW Cost	% Cost Increase
4gt4-v1_74*	46	47	-2.17
ham15_108	356	360	-1.12
one-two-three-v0_97	62	63	-1.61
one-two-three-v1_99	31	32	-3.23

Table 2 presents the results for a number of benchmark circuits from REVLIB. Our program applies the methods above to the circuit in both the forward and the reverse direction. A * after the circuit name indicates the addition of a single ancillary line because the circuit contains at least one MCT gate that uses all lines in the circuit.

The results are reported for each circuit for the better of the two directions. We report (1) the quantum cost from REVLIB, (2) the initial NCVW cost which is found by replacing MCT gates by the NCVW catalog circuits corresponding to Table 1, (3) the NCVW costs after MCT gate reduction is applied, (4) the NCVW cost after quantum gate expansion, (5) the NCVW cost after quantum gate reduction which is the NCVW cost of the final circuit, (6) the percentage cost reduction comparing the final NCVW cost to the REVLIB cost and (7) the CPU time for all steps. Overall, our methods yield a 44.9% improvement compared to the costs reported in REVLIB. The majority of the improvement (37.9%) comes from the catalog circuits. The rest comes from our quantum expansion and quantum reduction techniques.

Table 3 shows the four cases where the NCVW circuit is more costly than the NCV circuit. This results from the fact that our methods use many heuristics.

Table 4 shows the benchmarks for which the NCVW circuit is an improvement over the NCV circuit. The overall improvement for these examples is 4.71%.

As noted, our method adds an extra ancillary line if the MCT circuit includes a gate that uses all circuit lines. This is not the case for the results reported in REVLIB. However, the cost model employed in REVLIB is based on the work in Barenco *et al.* [1] which assumes a 2^{c-1}-th root-of-NOT gate is available to realize a c-control MCT gate in a circuit with $c+1$ lines. We anticipate that realizing gates progressively higher roots of NOT may be prohibitive in many technologies and adding one extra line will be preferable. Also we expect that synthesis methods can be made to avoid the situation in most cases.

6 Conclusions and Future Work

The benchmark results presented show that the methods described in this paper can lead to notably smaller quantum circuits than reported in REVLIB and other work. The results also show that using W and W^+ gates leads to smaller circuits than those using NCV gates. We thus conclude that the approach taken is quite promising and should be further refined.

Table 4. Benchmarks where NCVW circuit cost is less than NCV circuit cost

REVLIB Circuit	NCV Cost [8]	NCVW Cost	% Cost Reduction
4_49_16*	55	50	9.09
4gt10-v1_81	35	32	8.57
4gt12-v1_89*	37	36	2.7
4gt13_91	28	25	10.7
4gt4-v0_73*	49	48	2.04
4gt4-v0_78*	45	42	6.67
4gt4-v0_79*	41	38	7.32
4gt5_75	22	21	4.55
4gt5_76	27	26	3.7
4gt5_77	28	26	7.14
4mod7-v0_94	32	31	3.13
4mod7-v0_95	32	31	3.13
4mod7-v1_96	33	32	3.03
alu-v2_30*	103	98	4.85
alu-v2_31	83	78	6.02
alu-v2_32	38	35	7.89
alu-v4_36	28	27	3.57
cycle10_2_110	720	682	5.28
decod24-enable_126	77	75	2.6
decod24-v1_41*	23	20	13
decod24-v3_45*	35	31	11.4
ham15_107	1155	1107	4.16
ham15_109	198	190	4.04
ham7_104	84	76	9.52
ham7_105	64	59	7.81
hwb4_49*	54	49	9.26
hwb4_50*	54	49	9.26
hwb4_51*	73	71	2.74
hwb5_53*	282	270	4.26
hwb5_54*	234	220	5.98
hwb5_55	95	93	2.11
hwb6_56*	1150	1122	2.43
hwb6_57*	872	833	4.47
hwb6_58	132	127	3.79
hwb7_59*	3500	3352	4.23
hwb7_60*	2989	2829	5.35
hwb7_61*	2863	2731	4.61
hwb7_62*	1973	1878	4.82
hwb8_113*	10328	9787	5.24
hwb8_114*	8815	8378	4.96
hwb8_115*	8815	8378	4.96
hwb8_116*	4825	4496	6.82
hwb8_117*	4825	4496	6.82
hwb8_118*	10328	9787	5.24
hwb9_119*	28660	27340	4.61
hwb9_120*	28660	27340	4.61
hwb9_121*	28629	27311	4.6
hwb9_122*	28629	27311	4.6
hwb9_123*	14487	13434	7.27
mod5adder_127	104	102	1.92
mod5adder_128	84	80	4.76
mod5adder_129	76	74	2.63
one-two-three-v0_98	35	34	2.86
plus127mod8192_162*	35348	34178	3.31
plus63mod4096_163*	14652	13813	5.73
plus63mod8192_164*	19566	18856	3.63
rd53_130	195	191	2.05
rd53_135	59	58	1.69
rd53_136	59	58	1.69
rd53_137	59	58	1.69
sym6_145	212	199	6.13
sym9_148	672	659	1.93
Total	**265465**	**252958**	**4.71**

Our future work in this area will include extending the work to handle negative controls for MCT gates (controls that are activated by the value 0 and not 1). Other quantum gate libraries will be considered. We will also examine how various aspects of our methods and certain heuristics in particular might be changed to optimize the circuits even further. Lastly, except for the case of two controls, our procedure does not consider the permutation of MCT gate controls with a view to identifying more quantum gate reductions across MCT gate boundaries. We are considering how to address this. Exhaustive search is prohibitive and we have yet to determine how to identify which subset of the possible orderings will be most effective.

As noted above, two points on a line in a circuit which are assigned the same label by the line labeling procedure have the same functionality. The converse is not true, i.e. two points with the same functionality may be assigned different labels. As a result, our methods can miss certain reductions. We are investigating replacing the line labels with decision diagrams that will guarantee finding all functional equivalences. It remain to be seen whether the advantage gained will justify the added complexity and computational time.

References

1. Barenco, A., Bennett, C., Cleve, R., DiVincenzo, D., Margolus, M., Shor, P., Sleator, T., Smolin, J., Weinfurter, H.: Elementary gates for quantum computation. Physical Review A 52(5), 3457–3467 (1995)
2. Fredkin, E., Toffoli, T.: Conservative logic. Int'l J. of Theoretical Physics 21, 219–253 (1982)
3. Miller, D.M., Wille, R., Dueck, G.W.: Synthesizing reversible circuits from irreversible specifications using Reed-Muller spectral techniques. In: Proc. Reed-Muller Workshop, pp. 87–96 (May 2009)
4. Miller, D.M., Wille, R., Sasanian, Z.: Elementary quantum gate realizations for multiple-control Toffolli gates. In: Proc. Int'l Symp. on Multiple-valued Logic, pp. 288–293 (2011)
5. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge Univ. Press (2000)
6. Peres, A.: Reversible logic and quantum computers. Physical Review A 32, 3266–3276 (1985)
7. Sasanian, Z., Miller, D.M.: NCVW quantum gate realization of mixed control MCT gates. IEEE Trans. on CAD (2011) (submitted)
8. Sasanian, Z., Miller, D.M.: A new methodology for optimizing quantum realizations of reversible circuits. ACM J. on Emerging Technologies in Computing Systems (2011) (submitted)
9. Wille, R., Große, D., Teuber, L., Dueck, G.W., Drechsler, R.: RevLib: An online resource for reversible functions and reversible circuits. In: Int'l Symp. on Multi-Valued Logic, pp. 220–225 (2008), RevLib, `www.revlib.org`
10. Wille, R., Drechsler, R.: Synthesis of Boolean Functions in Reversible Logic. In: Progress in Applications of Boolean Functions (Synthesis Lectures on Digital Circuits and Systems). Morgan and Claypool (2010)
11. Wille, R., Große, D., Miller, D.M., Drechsler, R.: Equivalence checking of reversible circuits. In: Proc. Int'l Symp. on Multiple-valued Logic (CD), 7p (2009)